

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

**BRISCOE**

Atty. Ref.: 36-1518

Serial No. Unknown

Group:

National Phase of: PCT/GB00/02813

International Filing Date: 20 July 2000

Filed: December 26, 2001

Examiner:

For: DATA DISTRIBUTION

\* \* \* \* \*

December 26, 2001

Assistant Commissioner for Patents  
Washington, DC 20231

Sir:

**PRELIMINARY AMENDMENT**

Prior to calculation of the filing fee and in order to place the above identified application in better condition for examination, please amend as follows:

**IN THE SPECIFICATION**

Page 1, after the title insert the following:

-- This application is the US national phase of international application

PCT/GB00/02813 filed July 20, 2000 which designated the U.S. --.

**IN THE CLAIMS**

Please substitute the following amended claims for corresponding claims previously presented. A copy of the amended claims showing current revisions is attached.

3. (Amended) A method according to claim 1, in which step (d) includes combining values derived from a plurality of different seed values.

**BRISCOE**  
Serial No. **Unknown**

4. (Amended) A method according to claim 1, in which step (d) includes operating on a plurality of seed values with each of a plurality of different blinding functions.

9. (Amended) A method according to claim 1 in which the seed values are communicated to the user terminals, via a communications network.

14. (Amended) A method according to claim 1, in which each encrypted data unit carries an unencrypted index number to identify to any receiver which key in the sequence should be used to decrypt that data unit.

15. (Amended) A method according to claim 1 where the seeds required by any receiver to construct the keys for a specific sub-range of the entire key sequence are communicated in an order that implicitly identifies each seed.

16. (Amended) A method according to claim 1, in which multiple data senders use the same sequence of keys as each other to encrypt the same or different data units.

17. (Amended) A method according to claim 1, in which each key in the sequence generated from the seeds is used as an intermediate key to be combined with another intermediate key or sequence of keys to produce a sequence of keys to encrypt or decrypt the data units.

22. (Amended) A communications network comprising means arranged to operate in accordance with the method of claim 1.

24. (Amended) A network according to claim 22, in which the network includes a virtual private network (VPN) and in which different combinations of seeds for



**BRISCOE**  
Serial No. **Unknown**

**REMARKS**

Attached hereto is a marked-up version of the changes made to the claims by the current amendment. The attached page is captioned "**Version with markings to show changes made.**"

The above amendments are made to place the claims in a more traditional format.

Respectfully submitted,

**NIXON & VANDERHYE P.C.**

By:



**Larry S. Nixon**  
Reg. No. 25,640

**LSN:lmy**

1100 North Glebe Road, 8th Floor  
Arlington, VA 22201-4714  
Telephone: (703) 816-4000  
Facsimile: (703) 816-4100

**VERSION WITH MARKINGS TO SHOW CHANGES MADE**

3. (Amended) A method according to claim 1 [or 2], in which step (d) includes combining values derived from a plurality of different seed values.

4. (Amended) A method according to claim 1 [or 2 or 3], in which step (d) includes operating on a plurality of seed values with each of a plurality of different blinding functions.

9. (Amended) A method according to [any one of the preceding claims] claim 1 in which the seed values are communicated to the user terminals, via a communications network.

14. (Amended) A method according to [any of the preceding claims] claim 1, in which each encrypted data unit carries an unencrypted index number to identify to any receiver which key in the sequence should be used to decrypt that data unit.

15. (Amended) A method according to [any of claims 1 to 14] claim 1 where the seeds required by any receiver to construct the keys for a specific sub-range of the entire key sequence are communicated in an order that implicitly identifies each seed.

16. (Amended) A method according to [any of the preceding claims] claim 1, in which multiple data senders use the same sequence of keys as each other to encrypt the same or different data units.

17. (Amended) A method according to [any of the preceding claims] claim 1, in which each key in the sequence generated from the seeds is used as an intermediate key to be combined with another intermediate key or sequence of keys to produce a sequence of keys to encrypt or decrypt the data units.

**BRISCOE**  
Serial No. Unknown

22. (Amended) A communications network comprising means arranged to operate [by method] in accordance with the method of [any one of claims 1 to 19] claim 1.

24. (Amended) A network according to claim 22 [or 23], in which the network includes a virtual private network (VPN) and in which different combinations of seeds for constructing different sub-ranges of keys for decrypting data give members of the virtual private network different periods of access to the VPN.

25. (Amended) A data carrier storing a plurality of data units encrypted for use in a method according to [any one of claims 1 to 19] claim 1.